日本国特許庁
JAPAN PATENT OFFICE

25.09.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　９月３０日

出願番号
Application Number: 特願２００２－２８５１６８

[ST. 10/C]: [ＪＰ２００２－２８５１６８]

出願人
Applicant(s): ＦＤＫ株式会社

２００３年１０月３０日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０８９８６８

【書類名】　特許願

【整理番号】　IP02507

【あて先】　特許庁長官　殿

【国際特許分類】　G06F　7/58

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　山本　博康

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　アナンダ　ビターナゲ

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　清水　隆邦

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　藤田　香

【特許出願人】

【識別番号】　000237721

【氏名又は名称】　エフ・ディー・ケイ株式会社

【代理人】

【識別番号】　100067046

【弁理士】

【氏名又は名称】　尾股　行雄

【電話番号】　03-3543-0036

【選任した代理人】

【識別番号】　100096862

【弁理士】

【氏名又は名称】　清水　千春

【電話番号】　03-3543-0036

【手数料の表示】

【予納台帳番号】　008800

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　物理乱数の一様化手法

【特許請求の範囲】

【請求項１】　複数の物理乱数を乱数保持装置（２）に入力して保持し、この乱数保持装置に保持された物理乱数をその一部に基づいてランダムに選択して出力することを特徴とする物理乱数の一様化手法。

【請求項２】　複数の物理乱数を乱数保持装置（２）に入力して保持し、この乱数保持装置に保持された物理乱数をその一部に基づいてランダムに選択して出力する操作を１サイクルとし、

この操作を２サイクル以上繰り返して物理乱数を多段に一様化することを特徴とする物理乱数の一様化手法。

【請求項３】　乱数保持装置としてシフトレジスタ（２）を用いたことを特徴とする請求項１または請求項２に記載の物理乱数の一様化手法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、偏りのある物理乱数を簡単に一様化することが可能な物理乱数の一様化手法に関するものである。

【０００２】

【従来の技術】

一般に乱数には、計算によって決定論的に生成される擬似乱数と、自然界の物理現象を利用して生成される物理乱数とがある。後者（物理乱数）は真の意味でランダムな現象を基に生成されるので、理想的な乱数となる資質があるものの、実際に物理乱数を生成する場合、途中過程で様々な誤差要因が介在するため、必ずしも理想的な乱数が出力されるとは限らず、偏りのある乱数が出てきてしまう恐れもある。この誤差要因としては、デジタル化の際に基準となるクロックの幅や、ノイズを利用する場合に余計なノイズが混入することなどが挙げられる。

【０００３】

従来、こうした物理乱数の偏りを改善する手法、すなわち物理乱数の一様化手

法としては、２つの２進乱数を用いて乱数の偏りを改善するノイマンコレクター（例えば、非特許文献１参照）や、ノイズに基づいて発生させた物理乱数を擬似乱数と合成することで物理乱数の偏りを改善する手法（以下、乱数合成法と称する。）が提案されていた（例えば、特許文献１参照）。

【０００４】

【特許文献１】特開２００１－３４４０９４号公報（段落〔００１４〕〔００１８〕の欄、図１）

【非特許文献１】Benjamin Jun and Paul Kocher著、"The Intel Random Number Generator"、CRYPTOGRAPHY RESEARCH、１９９９年４月２２日発表（第４頁、4.3.Digital Post-Processing）

【０００５】

【発明が解決しようとする課題】

しかし、ノイマンコレクターでは、１ビットの乱数を出力するのに２ビットの乱数を必要とする上に、その２ビットの組合せによっては乱数を出力しない場合もあるので、乱数の発生速度が落ちてしまう欠点があった。

【０００６】

また、乱数合成法では、擬似乱数がわかれば、基になる物理乱数を出力から取り出せるようになるため、乱数の偏りが他人に知られてしまい、保安性に欠けるという不都合があった。

【０００７】

本発明は、このような事情に鑑み、乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供することを目的とする。

【０００８】

【課題を解決するための手段】

まず、本発明のうち請求項１に係る発明は、複数の物理乱数を乱数保持装置（２）に入力して保持し、この乱数保持装置に保持された物理乱数をその一部に基づいてランダムに選択して出力するようにして構成される。こうした構成を採用することにより、乱数保持装置に入力された物理乱数は、たとえそれが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に

知られてしまう事態が起きないように作用する。

【０００９】

また、本発明のうち請求項２に係る発明は、複数の物理乱数を乱数保持装置（２）に入力して保持し、この乱数保持装置に保持された物理乱数をその一部に基づいてランダムに選択して出力する操作を１サイクルとし、この操作を２サイクル以上繰り返して物理乱数を多段に一様化するようにして構成される。かかる構成により、物理乱数の一様化が一層促進されるように作用する。

【００１０】

さらに、本発明のうち請求項３に係る発明は、上記乱数保持装置としてシフトレジスタ（２）を用いて構成される。

【００１１】

なお、括弧内の符号は図面において対応する要素を表す便宜的なものであり、したがって、本発明は図面上の記載に限定拘束されるものではない。このことは「特許請求の範囲」の欄についても同様である。

【００１２】

【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

図１は本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の二例を示す回路図、

図２は本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の別の二例を示す回路図、

図３は本発明に係る物理乱数の一様化手法が適用される乱数一様化回路のさらに別の二例を示す回路図である。

【００１３】

まず、図１（ａ）に示す乱数一様化回路１では、シフトレジスタ２とセレクタ３とを具備しており、シフトレジスタ２のデータ端子Ｄには２進乱数（「０」または「１」）が順次入力され、シフトレジスタ２のクロック端子ＣＬＫに入力される基準パルス信号が立ち上がるごとに、これらの２進乱数が順に出力Ｑ００～Ｑ１３４にシフトされていく。そして、シフトレジスタ２の出力Ｑ００～Ｑ１２

７の１２８ビットの乱数はそれぞれセレクタ３のデータ端子Ｄ００～Ｄ１２７に入力され、シフトレジスタ２の出力Ｑ１２８～Ｑ１３４の７ビットの乱数はそれぞれセレクタ３のアドレスＡＤ０～ＡＤ６に入力される。

【００１４】

その後、セレクタ３では、アドレスＡＤ０～ＡＤ６に入力された７ビットのアドレス値に応じて、データ端子Ｄ００～Ｄ１２７に入力された１２８ビットの乱数から１ビットが選択され、出力端子ＯＵＴから出力される。例えば、アドレスＡＤ０～ＡＤ６にそれぞれ「１」「０」「０」「０」「０」「０」「０」が入力されたときは、データ端子Ｄ００に入力された乱数が出力端子ＯＵＴから出力される。また、アドレスＡＤ０～ＡＤ６にそれぞれ「１」「０」「１」「０」「０」「０」「０」が入力されたときは、データ端子Ｄ０４に入力された乱数が出力端子ＯＵＴから出力される。

【００１５】

このように、シフトレジスタ２のデータ端子Ｄに順次入力される２進乱数は、その一部がアドレスとなって自分自身をランダムに選び出すので、この２進乱数が偏りを持っていても、この乱数一様化回路１で一様化されて出力されることになる。しかも、従来のノイマンコレクターと異なり、１ビットの乱数を出力するのに複数ビットの乱数を必要とすることもなく、乱数を出力しない場合もないため、乱数の発生速度を維持することができる。また、従来の乱数合成法と違って、乱数の偏りが他人に知られてしまう事態が生じないので、保安性を確保することができる。

【００１６】

また、図１（ｂ）に示す乱数一様化回路１は、シフトレジスタ２からの乱数出力を選択するビット数を６ビットに減らしたことと、排他的論理和（ＸＯＲ）回路を追加したことを除き、図１（ａ）に示す乱数一様化回路１と同様である。すなわち、図１（ｂ）に示す乱数一様化回路１では、シフトレジスタ２とセレクタ３とを具備しており、セレクタ３の出力と２進乱数（「０」または「１」）とを入力とする排他的論理和回路の出力が順次シフトレジスタ２のデータ端子Ｄに入力され、シフトレジスタ２のクロック端子ＣＬＫに入力される基準パルス信号が

立ち上がるごとに、出力Ｑ００～Ｑ６９に順にシフトされていく。そして、シフトレジスタ２の出力Ｑ００～Ｑ６３の６４ビットの乱数はそれぞれセレクタ３のデータ端子Ｄ００～Ｄ６３に入力され、シフトレジスタ２の出力Ｑ６４～Ｑ６９の６ビットの乱数はそれぞれセレクタ３のアドレスＡＤ０～ＡＤ５に入力される。その後、セレクタ３では、アドレスＡＤ０～ＡＤ５に入力された６ビットのアドレス値に応じて、データ端子Ｄ００～Ｄ６３に入力された６４ビットの乱数から１ビットが選択され、出力端子ＯＵＴから出力される。

【００１７】

この場合も、シフトレジスタ２のデータ端子Ｄに順次入力される２進乱数は、その一部がアドレスとなって自分自身をランダムに選び出すので、この２進乱数が偏りを持っていても、この乱数一様化回路１で一様化されて出力されることになり、乱数の発生速度を維持すると同時に、保安性を確保することができる。

【００１８】

このことを確認するため、この乱数一様化回路１から出力された乱数の一様性を乱数検定規格ＦＩＰＳ１４０－２に準拠して評価した。その結果を表１および表２に示す。なお、表１中の数値は元データを表し、表２中の数値は検定結果データを表す。ここで、表１、２中の「Ｍｏｎｏ」、「Ｐｏｋｅｒ」、「Ｒｕｎｓ」および「ＬｏｎｇＲｕｎ」は乱数検定の種類を表しており、それぞれ乱数検定規格ＦＩＰＳ１４０－２の「Monobit Test」、「Porker Test」、「Runs Test」および「Long Run Test」に対応している。また、結果は５０回を１セットとして表示しており、数値は５０回の検定中で不合格になった回数を表している。

【表１】

セットNo.	Mono	Poker	Runs	LongRun
1	0	0	1	0
2	0	0	0	0
3	0	0	1	0
4	0	0	1	0
5	0	0	1	0
6	0	0	2	0
7	0	0	0	0
8	0	0	0	0
9	0	0	1	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	1	0
15	0	0	0	0
16	0	0	1	0
17	0	0	1	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	1	1
22	0	0	1	0
23	0	0	1	0
24	0	0	0	0
25	0	0	0	0
26	0	0	1	0
27	0	0	0	0
28	0	0	0	0
29	0	0	1	0
30	1	0	0	0
31	0	0	0	1
32	0	0	1	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	1
36	0	0	1	0
37	0	0	1	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	0	0
42	0	0	0	0
43	0	0	1	0
44	0	0	0	0
45	0	0	0	0
46	0	0	2	0
47	0	0	0	0
48	0	0	1	0
49	0	0	0	0
50	0	0	0	0

【表２】

セットNo.	Mono	Poker	Runs	LongRun
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	1	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0
27	0	0	0	0
28	0	0	0	0
29	0	0	0	0
30	0	0	0	0
31	0	0	0	0
32	0	0	0	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	0
36	0	0	0	0
37	0	0	0	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	1	0
42	0	0	0	0
43	0	0	0	0
44	0	0	0	0
45	0	0	0	0
46	0	0	0	0
47	0	0	0	0
48	1	0	0	0
49	0	0	0	0
50	0	0	0	0

【００１９】

表１、２から明らかなように、４種類すべての乱数検定（「Ｍｏｎｏ」、「Ｐｏｋｅｒ」、「Ｒｕｎｓ」および「ＬｏｎｇＲｕｎ」）において、セットNo.１～５０のほとんど全部が合格値となり、上述した効果が確認された。

【００２０】

一方、図２（ａ）に示す乱数一様化回路１は、シフトレジスタ２からの乱数出力を選択するビット数を１５ビットに増やしたことと、セレクタ３と同様な働きをするものとして論理積（ＡＮＤ）回路と排他的論理和（ＸＯＲ）回路との組み合わせを代用したことを除き、図１（ａ）に示す乱数一様化回路１と同様である。すなわち、図２（ａ）に示す乱数一様化回路１ではシフトレジスタ２を具備しており、シフトレジスタ２のデータ端子Ｄには２進乱数（「０」または「１」）が順次入力され、シフトレジスタ２のクロック端子ＣＬＫに入力される基準パルス信号が立ち上がるごとに、これらの２進乱数が順に出力Ｑ００～Ｑ３０にシフトされていく。そして、シフトレジスタ２の出力Ｑ００～Ｑ１４の１５ビットの乱数とシフトレジスタ２の出力Ｑ１６～Ｑ３０の１５ビットの乱数とを入力とする１５個の論理積回路の出力が、シフトレジスタ２の出力Ｑ１５とともに排他的論理和回路で順次合成されて出力される。

【００２１】

このように、シフトレジスタ２のデータ端子Ｄに順次入力される２進乱数は、シフトレジスタ２内で同じビット数（１５ビット）の２組に分けられた後、論理積回路と排他的論理和回路でランダムに演算されるので、この２進乱数が偏りを持っていても、この乱数一様化回路１で一様化されて出力されることになる。しかも、従来のノイマンコレクターと異なり、１ビットの乱数を出力するのに複数ビットの乱数を必要とすることもなく、乱数を出力しない場合もないため、乱数の発生速度を維持することができる。また、従来の乱数合成法と違って、乱数の偏りが他人に知られてしまう事態が生じないので、保安性を確保することができる。

【００２２】

また、図２（ｂ）に示す乱数一様化回路１は、シフトレジスタ２からの乱数出力を選択するビット数を７ビットに減らしたことと、排他的論理和（ＸＯＲ）回

路を追加したことを除き、図２（ａ）に示す乱数一様化回路１と同様である。すなわち、図２（ｂ）に示す乱数一様化回路１ではシフトレジスタ２を具備しており、シフトレジスタ２のデータ端子Ｄには２進乱数（「０」または「１」）が順次入力され、シフトレジスタ２のクロック端子ＣＬＫに入力される基準パルス信号が立ち上がるごとに、これらの２進乱数が順に出力Ｑ００～Ｑ１４にシフトされていく。そして、シフトレジスタ２の出力Ｑ００～Ｑ０６の７ビットの乱数とシフトレジスタ２の出力Ｑ０８～Ｑ１４の７ビットの乱数とを入力とする７個の論理積回路の出力が、シフトレジスタ２の出力Ｑ０７とともに排他的論理和回路で順次合成され、最後に元の２進乱数（生データ）と排他的論理和回路で合成されて出力される。

【００２３】

この場合も、シフトレジスタ２のデータ端子Ｄに順次入力される２進乱数は、シフトレジスタ２内で同じビット数（７ビット）の２組に分けられた後、論理積回路と排他的論理和回路でランダムに演算されるので、この２進乱数が偏りを持っていても、この乱数一様化回路１で一様化されて出力されることになり、乱数の発生速度を維持すると同時に、保安性を確保することができる。

【００２４】

なお、上述の実施形態においては、複数の物理乱数を保持する乱数保持装置としてシフトレジスタ２を用いた場合について説明したが、シフトレジスタ２以外の乱数保持装置（例えば、フリップフロップ）を代用することもできる。

【００２５】

また、上述の実施形態においては、１個の乱数一様化回路１を用いて物理乱数を一様化する場合について説明したが、図３に示すように、図１や図２に示す乱数一様化回路１を２個以上接続して物理乱数を多段に一様化することもできる。この場合、乱数一様化回路１の接続方法は、図３（ａ）に示すような直列接続であっても、図３（ｂ）に示すような並列接続であっても構わない。

【００２６】

【発明の効果】

以上説明したように、本発明によれば、乱数保持装置（シフトレジスタ）に入

力された物理乱数は、たとえそれが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に知られてしまう事態が起きないことから、乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供することができる。

【図面の簡単な説明】

【図１】

本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の二例を示す回路図である。

【図２】

本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の別の二例を示す回路図である。

【図３】

本発明に係る物理乱数の一様化手法が適用される乱数一様化回路のさらに別の二例を示す回路図である。

【符号の説明】

１……乱数一様化回路

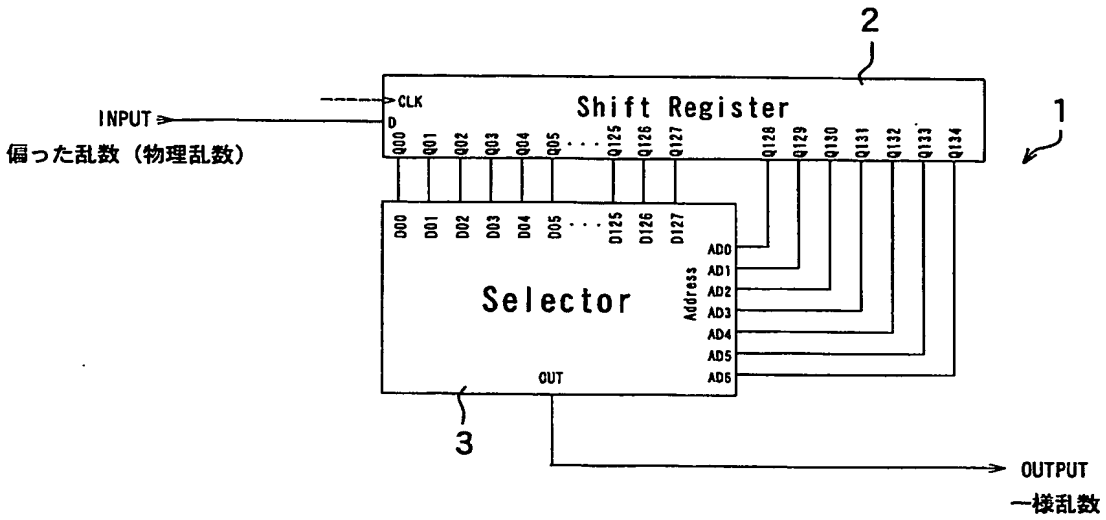
２……シフトレジスタ（乱数保持装置）

３……セレクタ

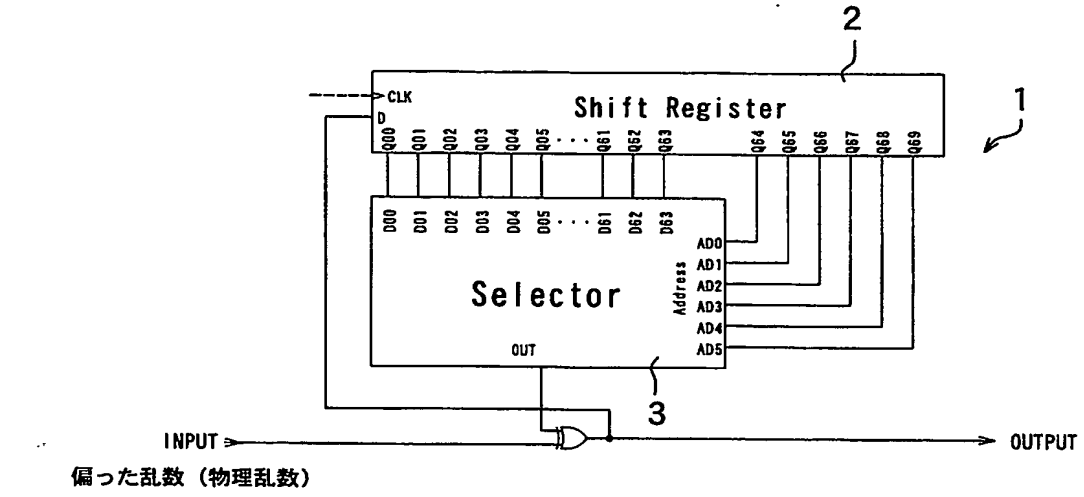
【書類名】　図面

【図１】

(a)

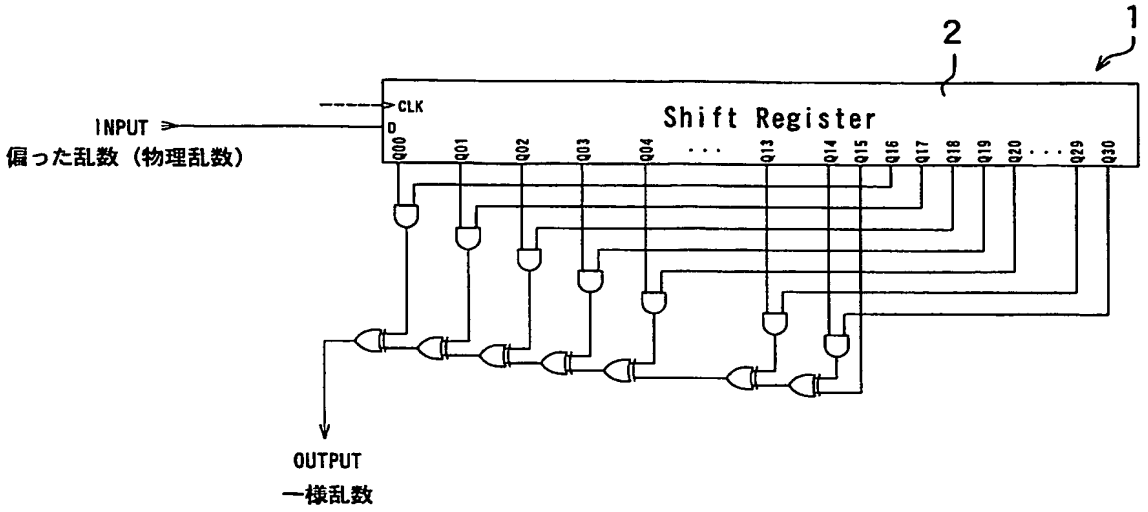

2
CLK
D
INPUT
偏った乱数（物理乱数）
Shift Register
Q00 Q01 Q02 Q03 Q04 Q05 ・・・ Q125 Q126 Q127 Q128 Q129 Q130 Q131 Q132 Q133 Q134
1
D00 D01 D02 D03 D04 D05 ・・・ D125 D126 D127
Selector
Address
AD0
AD1
AD2
AD3
AD4
AD5
AD6
OUT
3
OUTPUT
一様乱数

(b)

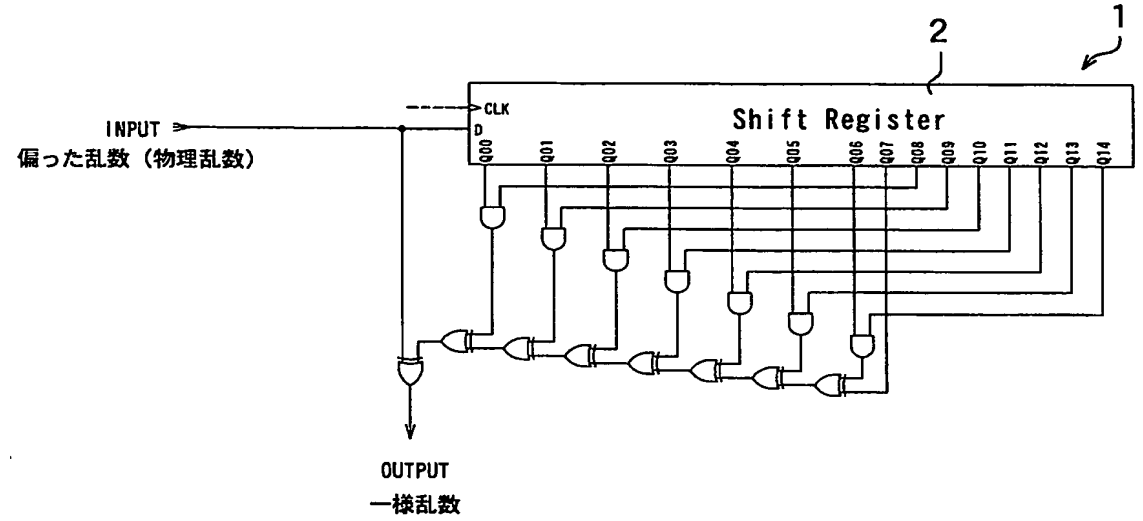

2
CLK
D
Shift Register
Q00 Q01 Q02 Q03 Q04 Q05 ・・・ Q61 Q62 Q63 Q64 Q65 Q66 Q67 Q68 Q69
1
D00 D01 D02 D03 D04 D05 ・・・ D61 D62 D63
Selector
Address
AD0
AD1
AD2
AD3
AD4
AD5
OUT
3
INPUT
偏った乱数（物理乱数）
OUTPUT

【図２】

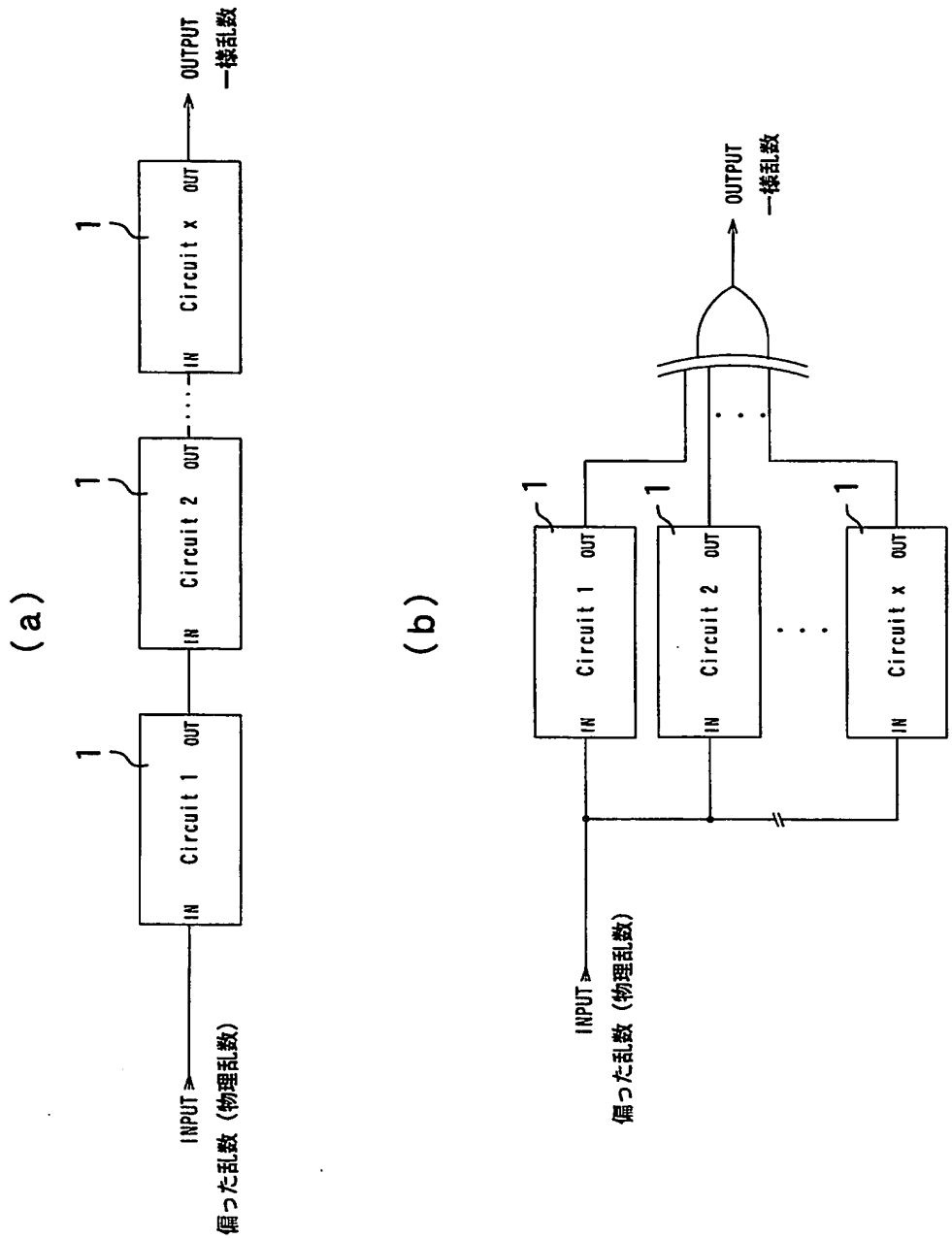
（ａ）


2
1
CLK
D
Shift Register
INPUT
偏った乱数（物理乱数）
Q00 Q01 Q02 Q03 Q04 ... Q13 Q14 Q15 Q16 Q17 Q18 Q19 Q20 ... Q29 Q30
OUTPUT
一様乱数

（ｂ）


2
1
CLK
D
Shift Register
INPUT
偏った乱数（物理乱数）
Q00 Q01 Q02 Q03 Q04 Q05 Q06 Q07 Q08 Q09 Q10 Q11 Q12 Q13 Q14
OUTPUT
一様乱数

【図３】


(a)
1
Circuit 1
IN
OUT
Circuit 2
Circuit x
INPUT
偏った乱数（物理乱数）
OUTPUT
一様乱数
(b)
Circuit 1
Circuit 2
Circuit x
INPUT
偏った乱数（物理乱数）
OUTPUT
一様乱数

【書類名】　要約書

【要約】

【課題】　乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供する。

【解決手段】　複数の物理乱数をシフトレジスタ２に順次入力して保持し、基準パルス信号が立ち上がるごとにシフトする。シフトレジスタ２に保持された物理乱数をその一部に基づいてセレクタ３でランダムに選択して出力する。これにより、シフトレジスタ２に入力された物理乱数は、それが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に知られる事態が起きない。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－２８５１６８
受付番号	５０２０１４６３０３３
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年１０月　１日

＜認定情報・付加情報＞

【提出日】　平成14年 9月30日

次頁無

特願２００２－２８５１６８

出　願　人　履　歴　情　報

識別番号　　［０００２３７７２１］

１．変更年月日　　２００１年　１月１６日
［変更理由］　名称変更
住　所　　東京都港区新橋５丁目３６番１１号
氏　名　　エフ・ディー・ケイ株式会社

２．変更年月日　　２００３年　８月１３日
［変更理由］　名称変更
住　所　　東京都港区新橋５丁目３６番１１号
氏　名　　ＦＤＫ株式会社